

Implementar una puerta de enlace FTDv en Azure mediante MCD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Registrar una aplicación](#)

[Crear un rol personalizado](#)

[Asignar el rol personalizado](#)

[Conectar la cuenta de Azure a MCD](#)

[Creación de una red virtual](#)

[Crear la puerta de enlace Azure MCD FTDv](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar los requisitos previos de Microsoft Azure e implementar una puerta de enlace de Firewall Threat Defence Virtual (FTDv) a través de MCD.

Prerequisites

- Una suscripción de Azure que se adquiere y registra, y que está asociada con el id. de Microsoft Entry. Confirme esto en la lista de Registros de aplicaciones en el portal de Azure.
- Función personalizada creada para la suscripción de Azure que concede acceso a Multicloud Defense (MCD) a los recursos y acciones específicos que, de lo contrario, se bloquearían.
- Una suscripción a Azure Event Grid, de modo que MCD pueda recibir actualizaciones en tiempo real desde la suscripción de Azure.
- La suscripción de Azure se conectó al controlador de defensa de la nube múltiple desde el panel de MCD.
- Los términos de Cisco Marketplace se aceptan en Azure, si es la primera vez que la cuenta de Azure se incorpora a MCD.

- (Opcional) Una identidad gestionada asignada por el usuario configurada, si necesita acceso a Key Vault o Blob Storage.
- Una nueva red virtual de servicios. Las redes virtuales que se crearon antes de que se introdujera la compatibilidad con el gateway FTDv no se pueden utilizar para una implementación de gateway FTDv.
- Una suscripción activa al centro de gestión de firewall en la nube (cdFMC), que gestiona la política de control de acceso para el dispositivo FTDv.
- Al menos una licencia de FTDv adquirida a través de su partner o vendedor de Cisco.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Exploración del portal de Microsoft Azure
- Registro de aplicaciones Microsoft Entry ID (Azure AD) y control de acceso basado en roles (RBAC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defence Virtual (FTDv)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

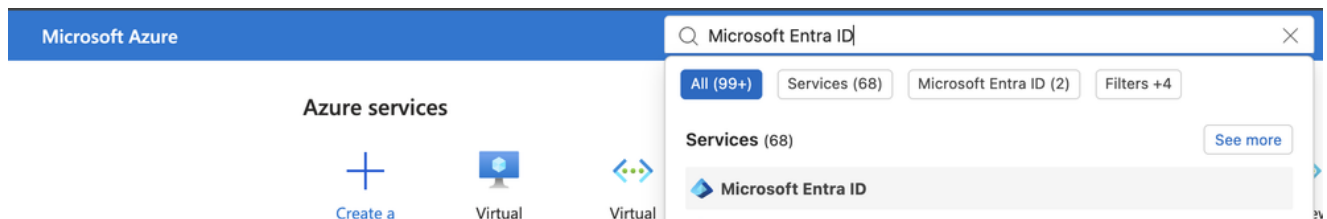
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

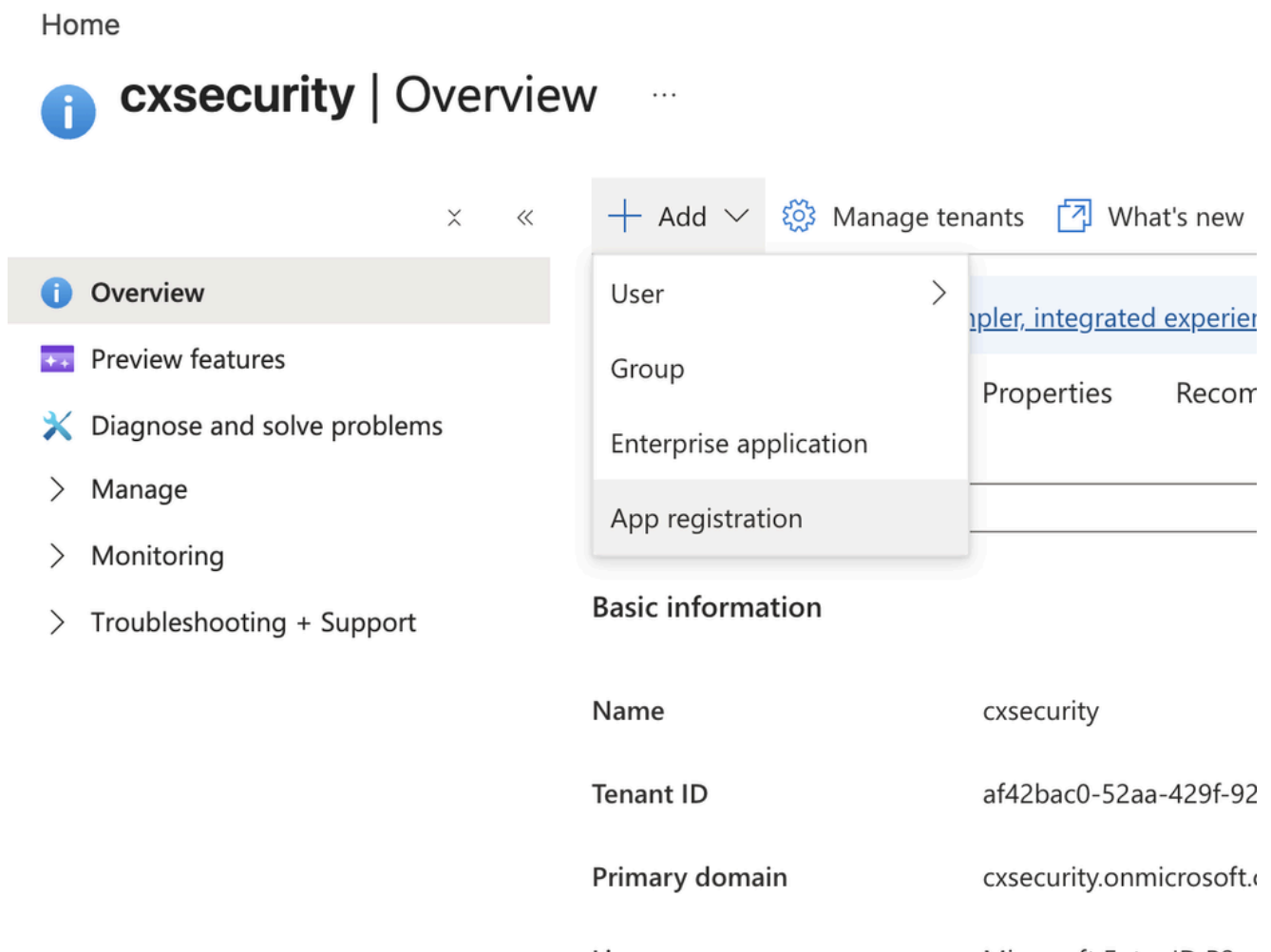
Utilice estos procedimientos para preparar Microsoft Azure, conectar su cuenta de Azure a MCD e implementar una puerta de enlace FTDv.

Registrar una aplicación

1. Navegue hasta Microsoft Entra ID con la barra de búsqueda del portal de Azure.



2. Haga clic en Agregar y seleccione Registro de aplicaciones.



3. En el formulario Registrar una solicitud, introduzca estos valores:

- Nombre: Un nombre fácilmente identificable para la aplicación.
- Tipos de cuenta admitidos: Seleccione la opción que mejor se adapte a su entorno. Este documento sólo utiliza arrendatario único.

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Choose the account types that can use this application or access this API

[Help me choose](#)

Communicating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

4. Para Redirigir URI (opcional), elija la opción adecuada para su entorno. Este documento no configura un URI de redireccionamiento.

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

5. Haga clic en Register.

6. Después de registrar la aplicación, aparece la página de descripción general. Copie y guarde la ID de aplicación (cliente) y la ID de directorio (arrendatario) en un bloc de notas.

The screenshot shows the 'Overview' page for the 'Multicloud Defense Controller' application. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, and Support + Troubleshooting. The main content area is titled 'Essentials' and displays the following information:

Property	Value	Action
Display name	Multicloud Defense Controller	
Application (client) ID	e5e0d63d-6f62-4f99-aaed-2eabd850cf72	Add a certificate or secret
Object ID	ec1746e4-bd16-4a00-aa7d-3b8e7e52496a	Add a Redirect URI
Directory (tenant) ID	a442bac0-52aa-429f-92db-925819967d17	Add an Application ID URI
Supported account types	My organization only	Managed application in L...
State	Activated	

Below the Essentials section, there are two informational messages:

- Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
- Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

At the bottom, there are links for 'Get Started' and 'Documentation'.

7. Desde la izquierda de la página de la aplicación, navegue hasta Administrar > Certificados y secretos.



Multicloud Defense Controller



Deactivate



Delete



Endpoints



Overview



Quickstart



Integration assistant



Diagnose and solve problems



Manage



Branding & properties



Authentication (Preview)



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles



Owners



Roles and administrators



Manifest

> Support + Troubleshooting

^ Essentials

Display name : [Multicloud Defense](#)

Application (client) ID : e5e0d63d-6f62-4ff

Object ID : ec1746e4-bd16-4a

Directory (tenant) ID : af42bac0-52aa-429

Supported account types : [My organization o](#)



Welcome to the new and improved App reg



Azure Active Directory Authentication Librai
Library (MSAL) and Microsoft Graph. [Learn i](#)

Get Started

Documentation

The Mi

8. Haga clic en New client secret.

Multicloud Defense Controller | Certificates & secrets ... Got feedback? Overview Quickstart Integration assistant Diagnose and solve problems

▼ Manage

 Branding & properties Authentication (Preview) **Certificates & secrets** Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest

> Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving to scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credent

 Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0)

Client secrets (0)

Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as

 New client secret

New client secret

Expires

Value ⓘ

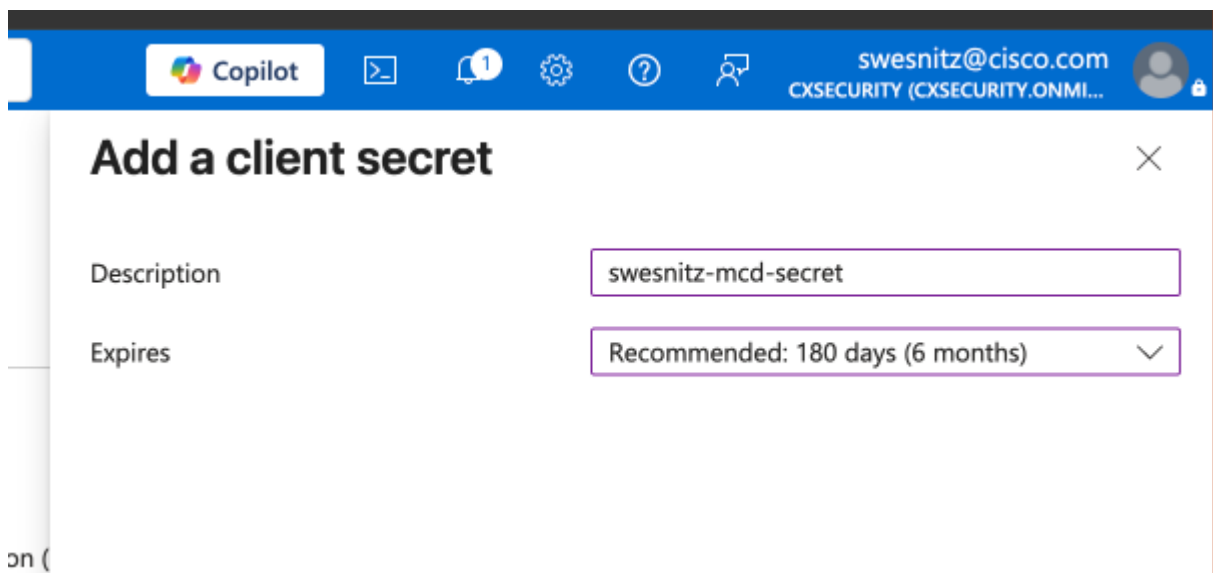
No client secrets have been created for this application.

9. En la página Add a client secret, introduzca estos valores y, a continuación, haga clic en Add:

- Descripción: Una descripción apropiada para el secreto de cliente.
- Caduca: En el menú desplegable, seleccione la opción que mejor se adapte a su entorno.



Nota: Debe crear un nuevo secreto cuando caduque el secreto actual.



Add a client secret

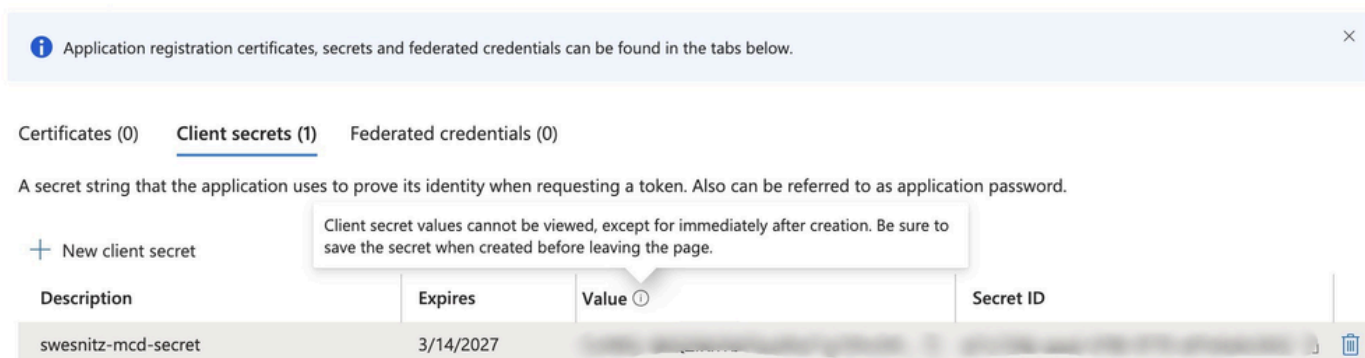
Description: swesnitz-mcd-secret

Expires: Recommended: 180 days (6 months)

10. Copie y guarde el Valor y el ID secreto en un bloc de notas.



Advertencia: Sólo puede ver el valor secreto en el momento de la creación.



Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.

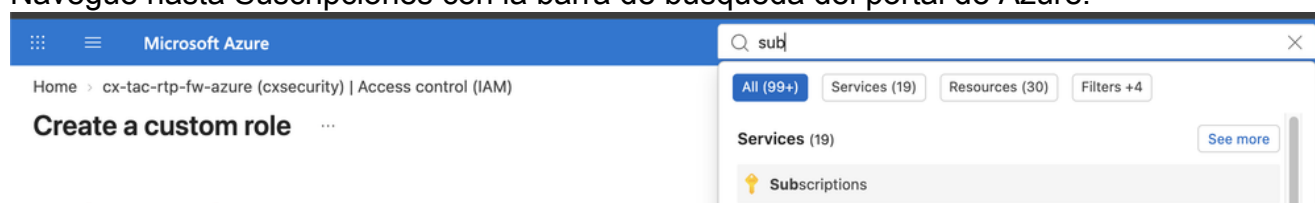
Description	Expires	Value	Secret ID
swesnitz-mcd-secret	3/14/2027		



Consejo: El secreto de cliente aparece en la columna Valor.

Crear un rol personalizado

1. Navegue hasta Suscripciones con la barra de búsqueda del portal de Azure.



Microsoft Azure

Home > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Create a custom role

sub

All (99+) Services (19) Resources (30) Filters +4

Services (19)

Subscriptions

2. Haga clic en su suscripción.

Home > Subscriptions

Subscriptions

cxsecurity (cxsecurity.onmicrosoft.com)

Compare the different Azure subscription types

Forecast my cost for next billing period

+ Add Manage Policies View Requests View eligible subscriptions Export to CSV Analyze

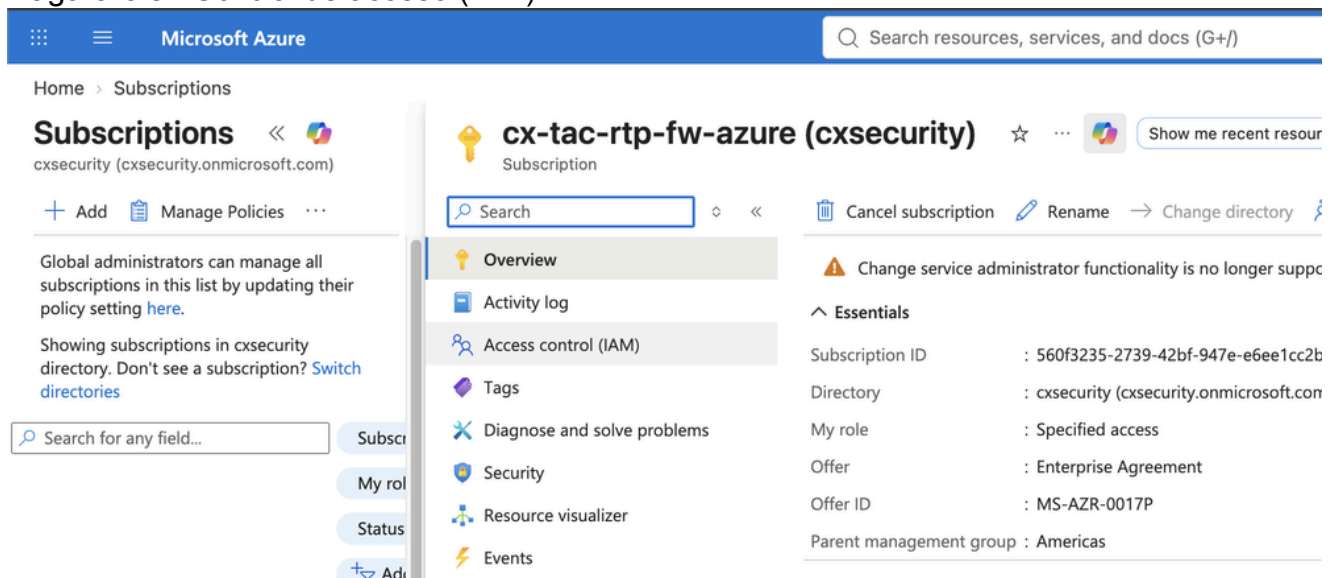
Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

Showing subscriptions in cxsecurity directory. Don't see a subscription? [Switch directories](#)

Search for any field... Subscriptions : **Filtered (1 of 1)** My role == all Status == all Add filter

☐ Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost
☐ cx-tac-rtp-fw-azure (cxsecurity)	560f3235-2739-42bf-947e-e6ee1cc2b999	Specified access	\$1,418.01

3. Haga clic en Control de acceso (IAM).



Microsoft Azure

Home > Subscriptions

Subscriptions

cxsecurity (cxsecurity.onmicrosoft.com)

+ Add Manage Policies ...

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

Showing subscriptions in cxsecurity directory. Don't see a subscription? [Switch directories](#)

Search for any field...

Subscriptions : **Filtered (1 of 1)** My role == all Status == all Add filter

cx-tac-rtp-fw-azure (cxsecurity) Subscription

Search

Cancel subscription Rename Change directory

Overview

- Activity log
- Access control (IAM)**
- Tags
- Diagnose and solve problems
- Security
- Resource visualizer
- Events

Essentials

Subscription ID : 560f3235-2739-42bf-947e-e6ee1cc2b

Directory : cxsecurity (cxsecurity.onmicrosoft.com)

My role : Specified access

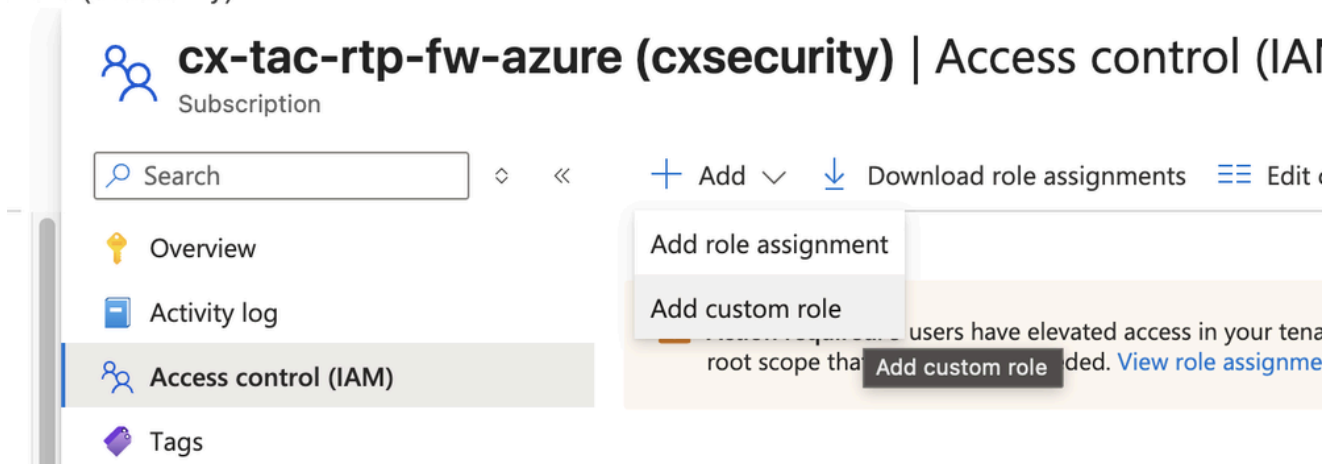
Offer : Enterprise Agreement

Offer ID : MS-AZR-0017P

Parent management group : Americas

4. Haga clic en Agregar y, a continuación, seleccione Agregar rol personalizado en el menú desplegable.

azure (cxsecurity)



cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Subscription

Search

+ Add Download role assignments Edit

Overview

Activity log

Access control (IAM)

Tags

Add role assignment

Add custom role

Add custom role

users have elevated access in your tenanted. [View role assignments](#)

5. Introduzca estos valores:

- Nombre de rol personalizado: Nombre fácilmente identificable para el rol personalizado.

- Descripción: Una descripción de la función.
- Permisos de línea base: Haga clic en el botón de opción Iniciar desde cero, si aún no está seleccionado.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Subscriptions > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Create a custom role

Basics

Permissions

Assignable scopes

JSON

Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name

Multicloud Defense-controller-role

Description

mcd azure test swesnitz

Baseline permissions

☐ Clone a role

☒ Start from scratch

☐ Start from JSON



Nota: El JSON que proporcione, no la ficha Permisos, asigna permisos a la función personalizada.

6. Haga clic en JSON.
7. Haga clic en Editar.
8. Pegue este bloque de código dentro de los corchetes para acciones:

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkInterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
```

```
"Microsoft.CognitiveServices/*/read",
"Microsoft.CognitiveServices/accounts/listkeys/action",
"Microsoft.Network/virtualHubs/*",
"Microsoft.Network/virtualHubs/hubRouteTables/*",
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/*",
"Microsoft.Authorization/roleAssignments/read",
"Microsoft.Authorization/roleDefinitions/read"
```

Home > Subscriptions > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Create a custom role ...

 If you change tabs and have unsaved edits, those changes will be discarded.

Basics Permissions **Assignable scopes** JSON Review + create

Here is your custom role in JSON format. [Learn more](#) 

Download



Discard changes

Save

```
1  {
2      "properties": {
3          "roleName": "Multicloud Defense-controller-role",
4          "description": "mcd azure test swesnitz",
5          "assignableScopes": [
6              "/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999"
7          ],
8          "permissions": [
9              {
10                 "actions": [],
11                 "notActions": [],
12                 "dataActions": [],
13                 "notDataActions": []
14             }
15         ]
16     }
17 }
```



Nota: Compruebe el espaciado y las tabulaciones correctos para el bloque de código JSON.

Este es un ejemplo de la definición de rol completada:

```
{
  "id": "/subscriptions/redacted/providers/Microsoft.Authorization/roleDefinitions/redacted",
  "properties": {
    "roleName": "Multicloud Defense-controller-role",
    "description": "mcd azure test swesnitz",
    "assignableScopes": [
      "/subscriptions/redacted"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.ApiManagement/service/*",
```

```

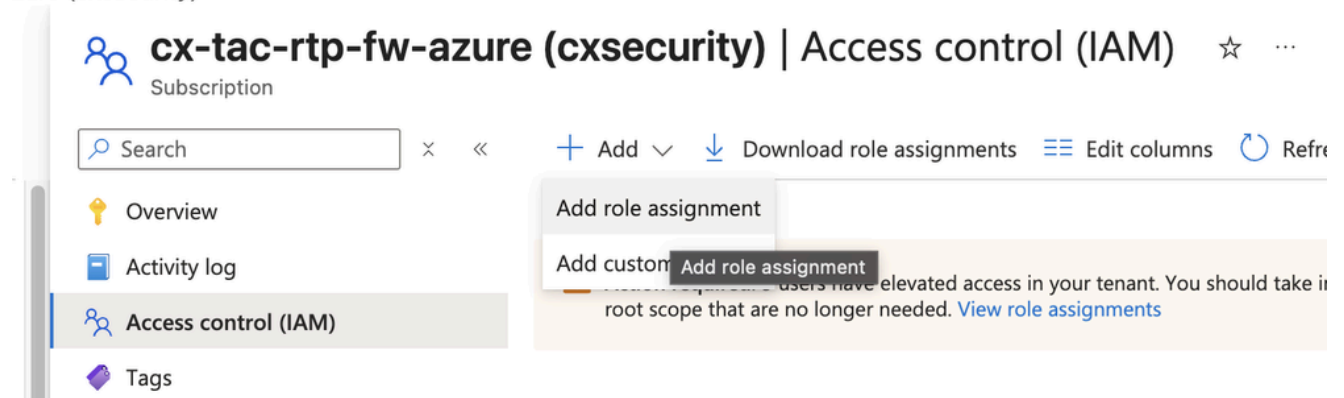
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkInterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.CognitiveServices/*/read",
...

```

Asignar el rol personalizado

1. En la página Control de acceso de suscripción (IAM), haga clic en Agregar asignación de rol.

zure (cxsecurity)



2. Busque el rol que ha creado en la sección Crear un rol personalizado.

Add role assignment ...

Role **Members** Conditions Assignment type Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)



Copilot can help pick a role

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Type : All

Category : All

Name ↑↓

Description ↑↓

Multicloud Defense-controller-role

mcd azure test swesnitz

Showing 1 - 1 of 1 results.

3. Haga clic en Next y deje Assign access (Asignar acceso) para establecer en User, group o service principal.

Add role assignment ...

Role **Members** Conditions Assignment type Review + assign

Selected role Multicloud Defense-controller-role

Assign access to
☒ User, group, or service principal
☐ Managed identity

Members + Select members

Name

Object ID

Type

No members selected

Description

Optional

4. Haga clic en Seleccionar miembros.

Add role assignment ...

Role **Members** Conditions Assignment type Review + assign

Selected role Multicloud Defense-controller-role

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

Name	Object ID	Type
------	-----------	------

No members selected

Description

5. Agregue el rol que creó en la sección Crear un rol personalizado.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Haga clic en Next y, a continuación, copie la ID de suscripción.

Add role assignment

Role Members Conditions Assignment type Review + assign

 If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

Role	Multicloud Defense-controller-role		
Scope	/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999		
Members	Name	Object ID	Type
	Multicloud Defense Controller	309bad3d-eb32-4c16-b2bb-0289b3d491f6	App
Description	No description		
Assignment type	Active		
Assignment duration	Permanent		

7. Haga clic en Revisar + asignar.

Add role assignment ...

Role Members Conditions Assignment type Review + assign

 If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

Role	Multicloud Defense-controller-role	
Scope	/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999	
Members	Name	Object ID
	Multicloud Defense Controller	309bad3d-eb32-4c16-b2bb-0289b3d491f6
Description	No description	
Assignment type	Active	
Assignment duration	Permanent	

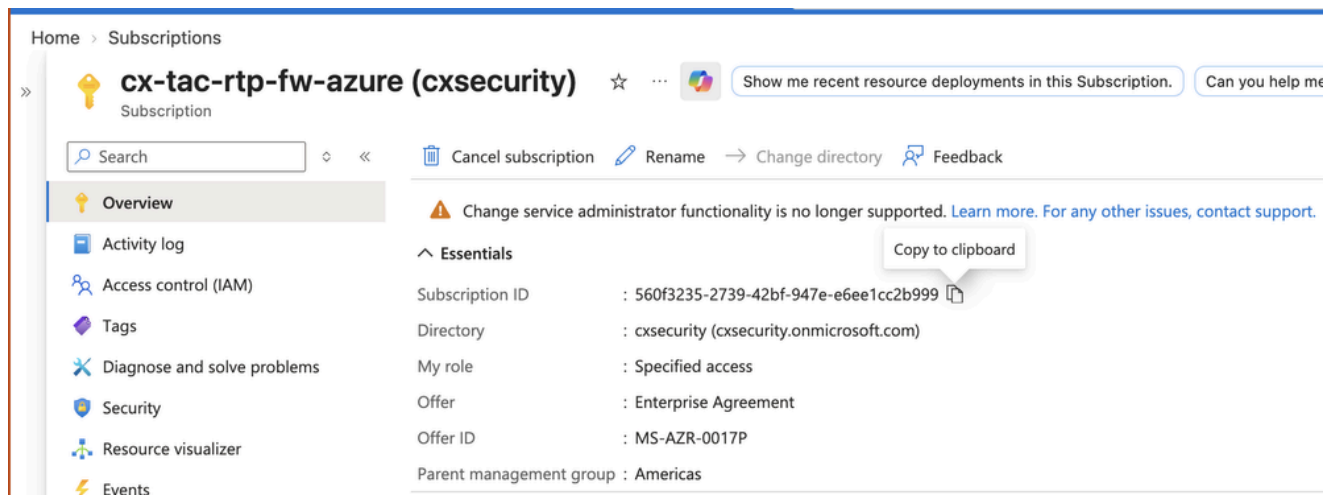
Review + assign

Review + assign

Previous

Next

8. Aparecerá la página de descripción general de la suscripción. En el menú de la izquierda, vaya a Overview y copie la ID de suscripción.



Esto completa los requisitos previos de Azure para agregar la cuenta de Azure a MCD. Estos procedimientos describen la integración y la implementación a través de MCD.

Conectar la cuenta de Azure a MCD

1. Vaya a SCC > Defensa de la nube múltiple.



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



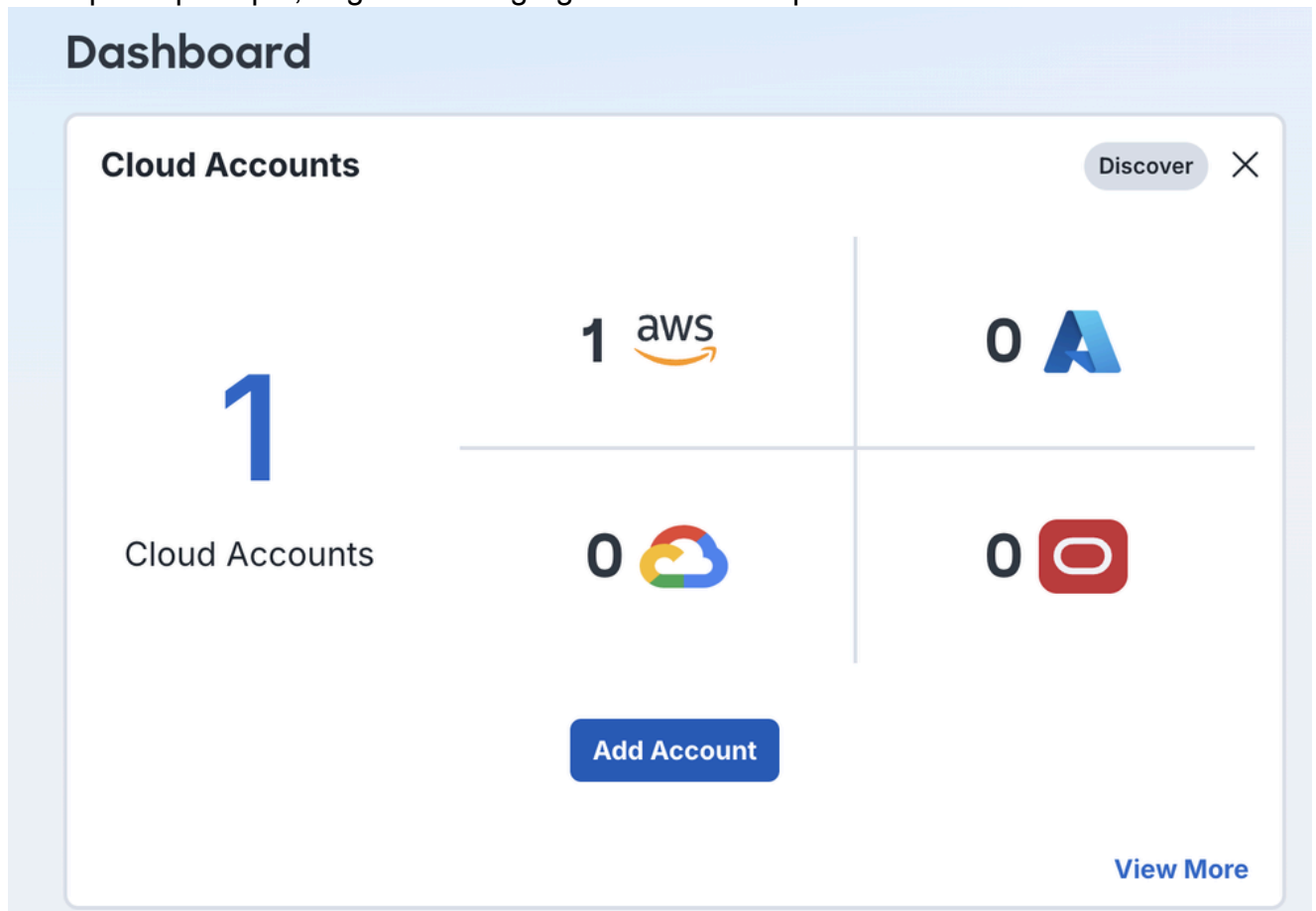
Security Devices



Platform Management



2. En el panel principal, haga clic en Agregar cuenta en el panel Cuentas en la nube.



3. Haga clic en el icono Azure.

Select Your Cloud Account
Please select Account Type you want to set up









[Close](#)[Back](#)

4. En la página Connect Your Azure Account, ingrese estos valores:
- Nombre de cuenta de Azure: El nombre de la cuenta de Azure desde la perspectiva de MCD.
 - ID de directorio: El ID de directorio que guardó en la sección Registrar una aplicación.
 - ID de suscripción: El ID de suscripción que guardó en la sección Asignar el rol personalizado.
 - ID de aplicación: El ID de aplicación que guardó en la sección Registrar una aplicación.
 - Secreto de cliente: Valor que ha guardado en la sección Registrar una aplicación.

Connect Your AZURE Account

Prepare your cloud account for integration with Cisco Multicloud Defense Controller with following steps:



- 1 Open up [Azure Cloud Shell](#) in bash mode.
- 2 Download and execute Cisco Multicloud Defense onboarding script in the bash shell. This script creates an App Registration for Cisco Multicloud Defense Controller.
Click [here](#) to see the privilege for the App created.

[Copy](#)

```
bash <( curl -Ls https://raw.githubusercontent.com/valtix-security/cli-azure-setup/master/azure-setup.  
sh ) -w "https://prod1-webhook.mcd.us.cdo.cisco.com:8093/webhook/ciscoswesnitz-US_htztw/azure"
```

Azure Account Name * ⓘ

Description ⓘ

Directory ID * ⓘ

Subscription ID * ⓘ

Application ID * ⓘ

Client Secret * ⓘ

[Show](#)

Cancel

Back

Next

5. MCD detecta y muestra los recursos de Azure. Haga clic en Next (Siguiente).

Discovering Assets

Doing our magic to discover all of your assets. Please give us a minute...

1
Cloud Accounts

63
Regions

-
Network ACL

-
Network ACL Rules

-
Application Security Groups (Azure)

-
AI Inventory

-
VPCs/VNets

-
Subnets

-
Security Groups

-
Load Balancers

-
Instances

-
Network Interfaces

-
Tags

-
Route Tables

-
Applications

-
Certificates

Cancel

Back

Next

6. Haga clic en Close (Cerrar).

Success!

Now that you have added an account, you can take full advantage of our feature set to view traffic and secure your VPCs and VNETs.

Step 1

Connect Account



Connect a cloud account with the Multicloud Defense Controller

Connect Account

Step 2

Enable Traffic Visibility



Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Step 3

Secure Your Account

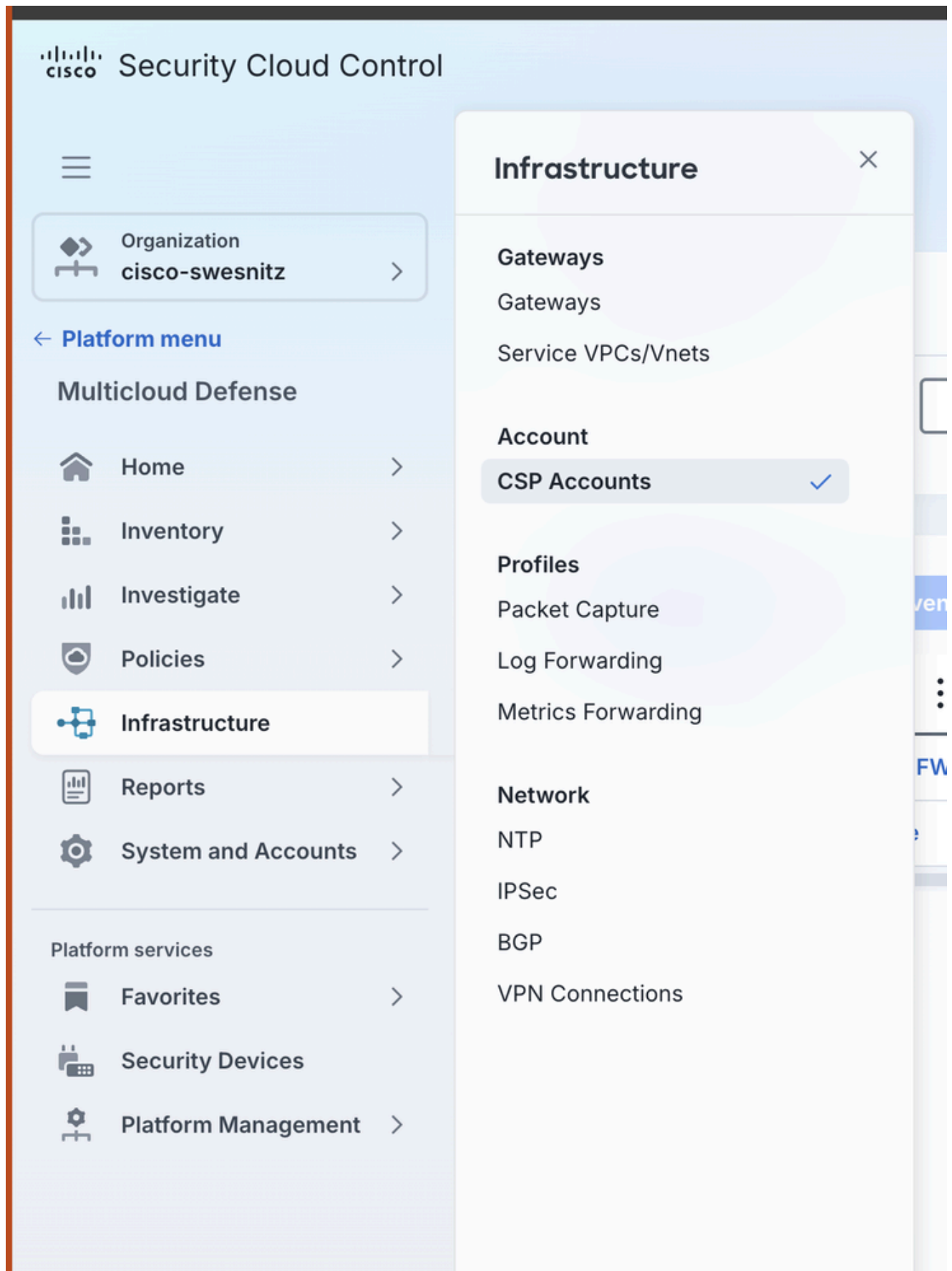


Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

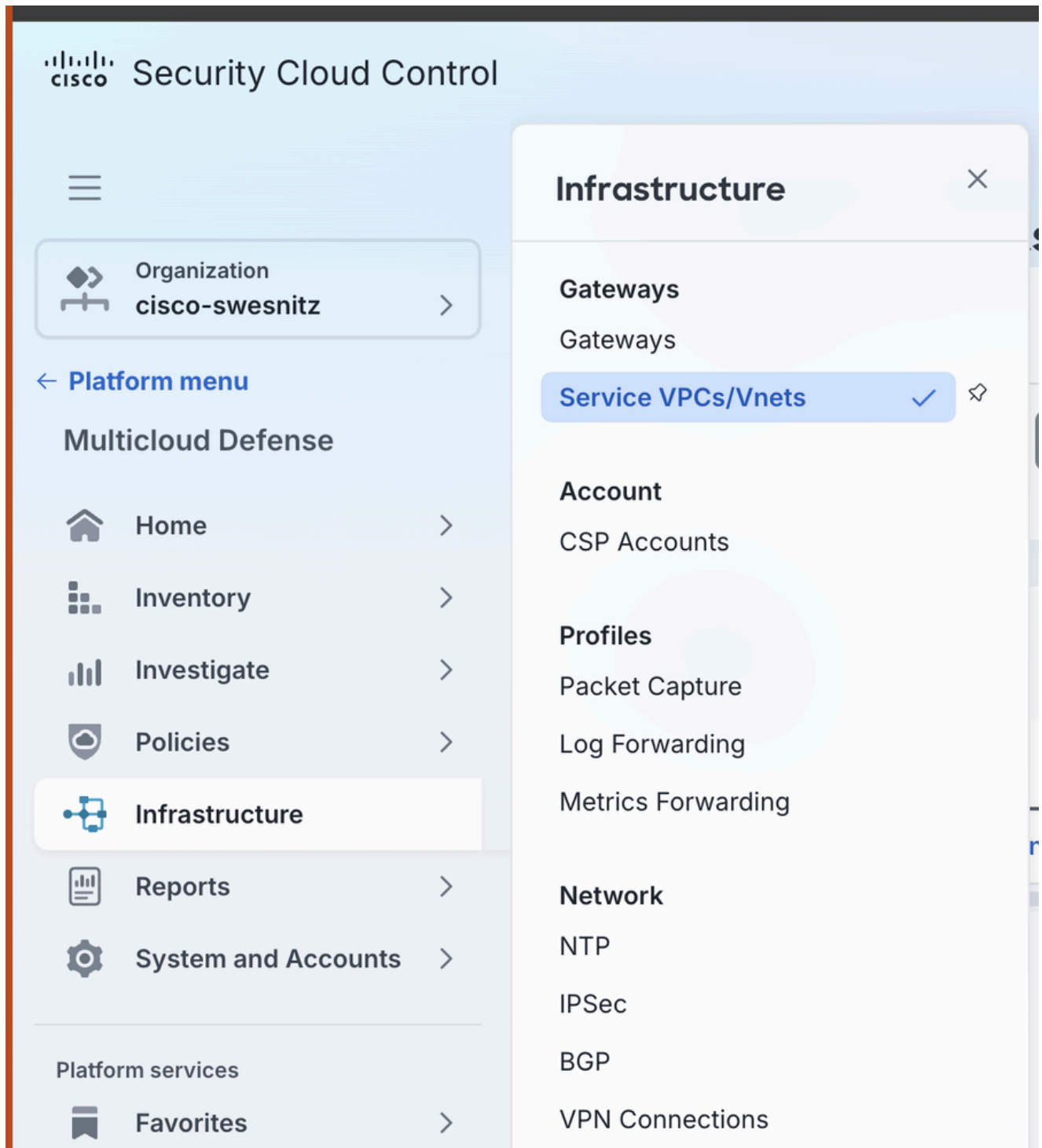
CloseBack

7. Ahora puede ver la cuenta incorporada desde Infrastructure > CSP Accounts.



Creación de una red virtual

1. Vaya a Infrastructure > Service VPCs/VNets.



2. Haga clic en Crear.

Service VPCs/VNets: 1

Quick Filters

Advanced

Name



All Accounts



CSP Type

Create

Actions



Name



ID



Account



mcd_test_vpc-swesnitz

1

AWS-CXLABS-RTP-FW

3. Introduzca estos valores:

- Nombre: Nombre fácilmente identificable para la VNet que este procedimiento crea para la puerta de enlace FTDv.
- Cuenta CSP: El nombre que asignó en la sección Conectar la cuenta de Azure a MCD.
- Región: Región en la que se implementa la puerta de enlace FTDv.
- Bloque CIDR: Un bloque IP único para la gateway de tránsito asociada a la VNet.
- Zonas de disponibilidad: Seleccione al menos dos zonas de disponibilidad para la resistencia.
- Grupo de recursos: Seleccione + Create Resource Group en el menú desplegable.
- Nombre del grupo de recursos: Nombre del grupo de recursos.
- Región Grupo de Recursos: Región que se alinea con la región seleccionada para Región.

Click Save.

Create Service VPC



Name * ⓘ

mcd_azure_vnet

CSP Account * ⓘ

cx-tac-rtp-fw-azure

Region * ⓘ

East US eastus

CIDR Block * ⓘ

10.4.0.0/16

Availability Zones * ⓘ

☒ 1

☒ 2

☐ 3

Resource Group *

+ Create Resource Group

Resource Group Name *

mcd_swesnitz

Resource Group Region *

East US eastus

☐ Use NAT Gateway ⓘ

vWAN Attachment

☐ Enable vWAN Attachment

Cancel

Save

4. Aparece un mensaje de confirmación.

 **Success**

Service VPC/VNet created successfully.

OK

Confirme la creación de VNet desde el lado de Azure, navegue hasta Network foundation > Virtual networks overview > Virtual Networks.

Home > Network foundation

Network foundation | Virtual Network overview

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Virtual network

Network foundation

Service to provision private networks. Build an isolated, secure environment to run virtual machines (VMs) and applications.

Enhanced security through isolated, secure environments.

Flexible, scalable without physical changes.

Secure connectivity across Azure regions

Learn more

Create

View resources

Connectivity

Home > Network foundation

Network foundation | Virtual networks

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Create

Manage view

Refresh

Export to CSV

Open query

mcd

Subscription equals all

Resource Group equals all

Name ↑

mcd_test_vnet-swesnitz

La VNet pasa a un estado Activo una vez que se ha creado.

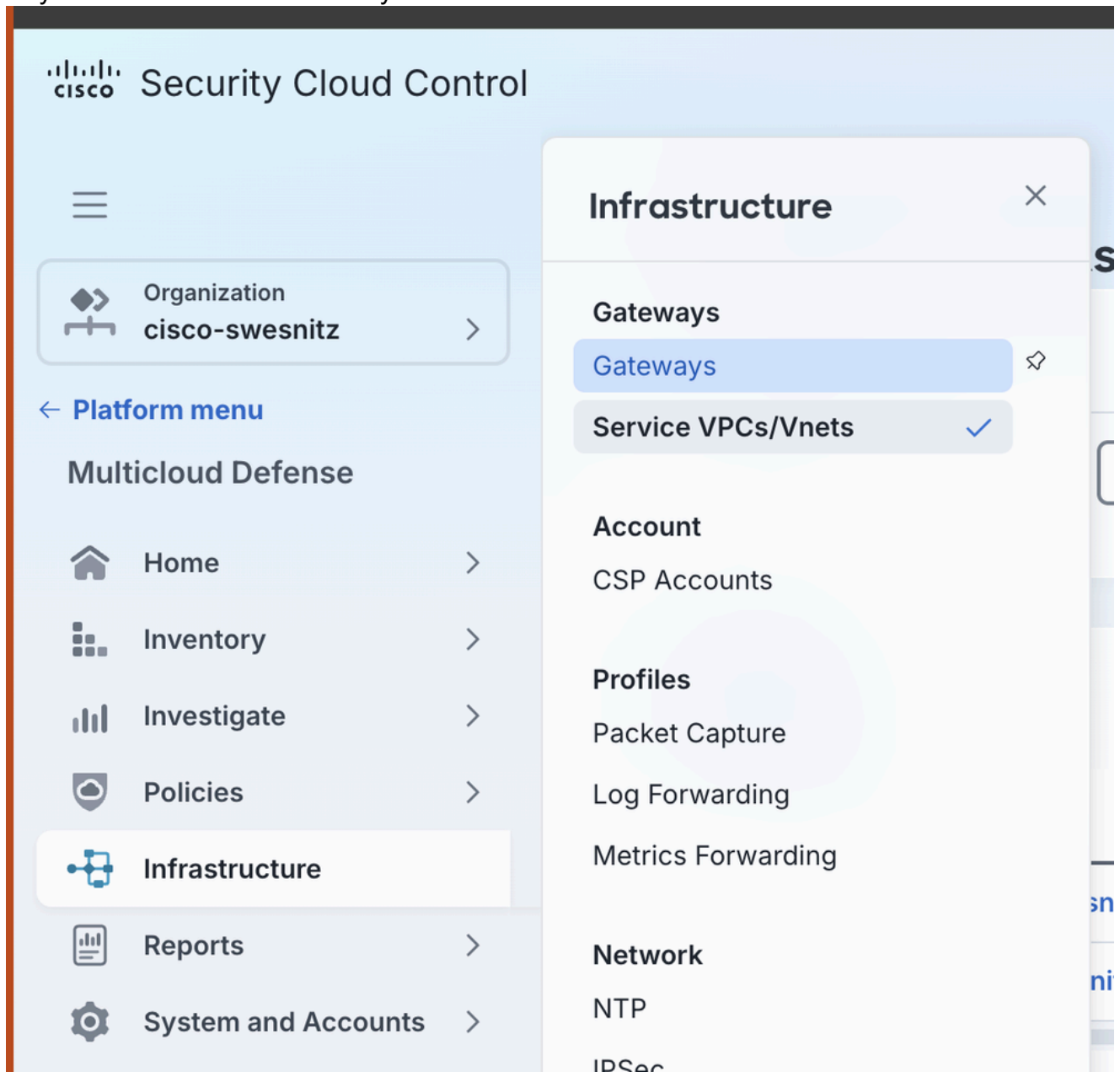
CreateActions

Refresh

☐	Name	ID	Account	CSP Type	Region	State
☐	mcd_test_vnet-swesnitz	2	cx-tac-rtp-fw-azure	AZURE	eastus	ACTIVE

Crear la puerta de enlace Azure MCD FTDv

1. Vaya a Infrastructure > Gateways.



2. Haga clic en Add Gateway.

The screenshot displays the Cisco Security Cloud Control web interface. On the left is a navigation sidebar with a 'Platform menu' containing options like Home, Inventory, Investigate, Policies, and Infrastructure. The main content area is titled 'Gateways: 1' and includes filter tabs for 'Quick Filters' and 'Advanced'. Below these are input fields for 'Name' and 'CSP Account'. A table at the bottom lists gateways with columns for selection, Name, and State. One gateway is visible with the name 'med lab cluster' and state 'ACTIVE'.

3. Introduzca estos valores:

- Cuentas: En el menú desplegable, seleccione la cuenta de Azure que vinculó en la sección Conectar la cuenta de Azure a MCD.
- Tipo de gateway: Seleccione FTDv Gateway.
- Nombre: Nombre fácilmente identificable para la puerta de enlace FTDv.
- Tipo de instancia: El tipo de instancia apropiado para su entorno.
- Instancias mínimas: Seleccione al menos una instancia en el menú desplegable.
- Instancias máximas: El número máximo de instancias de FTDv que desea para su entorno. El máximo permitido es 10.
- Puerto HealthCheck: El valor predeterminado es 65534. Este documento no modifica este valor.

Create Gateway

Gateway InformationGateway DetailsAdvanced SettingsReview

Properties

Accounts * ⓘ

cx-tac-rtp-fw-azureX v

Gateway Type *

FTDv GatewayX v

Name * ⓘ

mcd-azure-labX

Description

Optional

Instance Type * ⓘ

8 Virtual CPU | AZURE_D8S_V5X v

Minimum Instances * ⓘ

1v

Maximum Instances * ⓘ

3v

HealthCheck Port * ⓘ

65534X

Cancel

Next



Nota: El puerto HealthCheck es el número de puerto que el equilibrador de carga de Defensa de varias nubes utiliza para comprobar el estado de las instancias. Los grupos de seguridad de ruta de datos asignados a las instancias deben permitir el tráfico en este puerto.

4. Introduzca estos valores:

- Propiedades: Seleccione Egress o East-West.
- Versión de FTDv: La versión de software más adecuada para el entorno.
- Conjunto de reglas de política: La política de control de acceso (ACP) que se aplicará

a este clúster FTDv.

- Contraseña Una contraseña para las instancias de FTDv.
- Modelo de licencia: El modelo de licencia deseado.
- Nivel de rendimiento: El nivel adecuado para el rendimiento esperado del dispositivo.
- Tipos de licencias: Los tipos de licencia adquiridos para esta implementación.
- Región: La región en la que se despliegan estas instancias de FTDv.
- ID de VPC/VNet: La red virtual de servicio que ha creado en la sección Crear una red virtual.

Create Gateway

Security * ⓘ

East West ×

FTDv Version *

10.0.0 ×

Policy Ruleset * ⓘ

Default Access Control Policy ×

FTDv

Admin Password

..... × Show

Password Requirements:

- Must be between 12 and 72 characters long
- Use lowercase and uppercase characters, and numbers
- At least one special character (excluding \ and -)
- No more than 2 repeating or sequential characters

License Model ⓘ

Smart Licensing Multicloud Defense

Performance Tier * ⓘ

FTDv20

License Types * ⓘ

Base ×

Location

Region *

East US eastus ×

VPC/VNet ID * ⓘ

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz ×

Key Selection

Cancel

Back

Next

5. Cree un par de claves públicas. Consulte [Creación de un Par de Llaves SSH en Windows](#) para obtener ayuda.

```

Your cloud shell session will be ephemeral so no files or system changes will
shelby [ ~ ]$ ssh-keygen -m PEM -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/shelby/.ssh/id_rsa):
Created directory '/home/shelby/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shelby/.ssh/id_rsa
Your public key has been saved in /home/shelby/.ssh/id_rsa.pub
The key fingerprint is:

```

6. Introduzca los valores para SSH Public Key y Resource Groups.

Create Gateway

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/9UG6Cg6R0O
IXvmuK/DY2UcDm/P0CFeww/cKCMToG6Ogx8IK/M

Resource Groups *

mcd_swesnitz | eastus

User Assigned Identity ID ⓘ

Enter User Assigned Identity ID

Mgmt. Security Group * ⓘ

mcd_test_vnet-swesnitz-mgmt-sg | mcd_swesnitz

Datapath Security Group 1 * ⓘ

mcd_test_vnet-swesnitz-datapath-sg | mcd_sw...

Datapath Security Group 2 *

mcd_test_vnet-swesnitz-second-datapath-sg | ...

Disk Encryption * ⓘ

Azure managed encryption

Instance Details

You can only modify availability zones for gateways deployed in edge mode for GCP, Azure, and OCI environments

Availability Zone ↻

Mgmt. Subnet ↻

Datapath Subnet 1

Datapath Subnet 2

1
mcd test vnet-...
mcd test vne...
mcd test vne...

Cancel

Back

Next

7. Inhabilite la IP pública y haga clic en Next.

Create Gateway

✓

✓

3

4

Gateway InformationGateway DetailsAdvanced SettingsReview

Public IP

☒ Disable Public IP

8. Revise todos los valores especificados.

Create Gateway

Gateway Information

Edit

Name

mcd-azure-lab

Gateway Type

FTDv Gateway

Min Instances

1

Max Instances

3

HealthCheckPort

65534

Policy Ruleset ID

Default Access Control Policy

Property

East West

Instance Type

AZURE_D8S_V5

FTDv Version

10.0.0

Gateway Details

Edit

License Model

Smart Licensing

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd_swesnitz

Mgmt. Security Group

mcd_test_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd_test_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd_test_vnet-swesnitz-second-datapath-sg

Cancel

Back

Finish

9. Después de revisar los valores y de finalizar la carga de los recursos, haga clic en Finalizar.

Create Gateway

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd_swesnitz

Mgmt. Security Group

mcd_test_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd_test_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd_test_vnet-swesnitz-second-datapath-sg

EBS Encryption

AZURE EBS encryption key

Instance Details

Availability Zone	Mgmt. Subnet	Datapath Subnet 1	Datapath Subnet 2
1	mcd_test_vnet-swesnitz-mgmt-1	mcd_test_vnet-swesnitz-datapath-1	mcd_test_vnet-swesnitz-second-datapath-1
2	mcd_test_vnet-swesnitz-mgmt-2	mcd_test_vnet-swesnitz-datapath-2	mcd_test_vnet-swesnitz-second-datapath-2

Recommendations

loading...

Resources Info

loading...

Advanced Settings

Edit

Disable Public IP

enabled

Cancel

Back

Finish

Vista de panel una vez cargados los recursos.

Instance Details

Availability Zone	Mgmt. Subnet	Datapath Subnet 1	Datapath Subnet 2
1	mcd_azure_vnet-mgmt-1	mcd_azure_vnet-datapath-1	mcd_azure_vnet-second-datapath-1
2	mcd_azure_vnet-mgmt-2	mcd_azure_vnet-datapath-2	mcd_azure_vnet-second-datapath-2

Resources Info



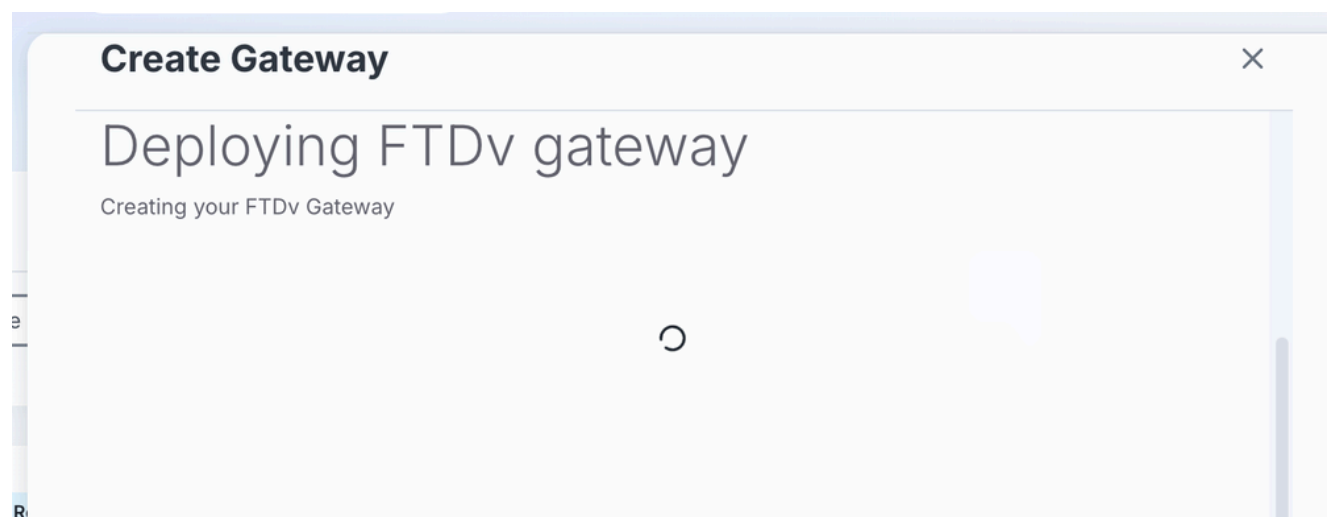
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

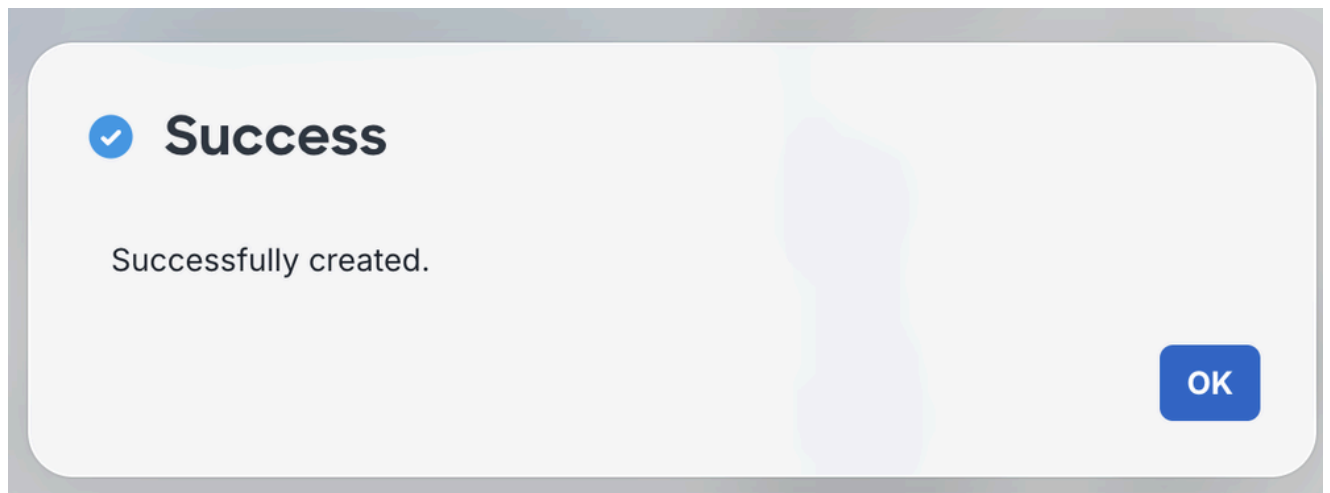
[Edit](#)**Disable Public IP**

enabled

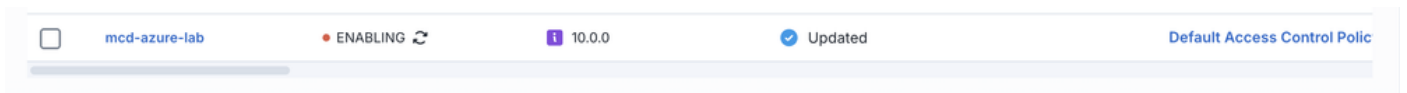
Vista del panel de la implementación del gateway.



10. Cuando la puerta de enlace comienza a crearse, aparece un mensaje de operación correcta. Click OK.



En el panel de MCD, el estado muestra ENABLING.



Controle el estado desde las pestañas Summary e Instances.

Details

Edit

Actions

✕

Summary

Cloud Details

Interfaces

Instances

Settings

Troubleshooting

Terraform

Name

mcd-azure-lab

State

ENABLING

Description

Instance Type

AZURE_D8S_V5

Type

FTDv Gateway

Min/Max Instances

1 / 3

Mode

HUB

Security Type

East West

Policy Rule Set

Default Access Control Policy

FTDv Version

10.0.0

License Model

Smart Licensing

Performance Tier

FTDv20

License Types

Base

Date Created (Local)

2026-09-15 16:22:37.053

Last Modified (Local)

2026-09-15 16:23:32.156

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

- En Compute > Virtual machines en Azure, monitoree las instancias de FTDv. El estado cambia de Creación a En ejecución.

Home

Compute infrastructure

Compute infrastructure

Virtual machines

Identify VMs with network connectivity issues

Analyze alerts across virtual machines

Get workload templates for VMs

Search

Virtual machines

Get started

Overview

All resources

Infrastructure

Virtual machines

Virtual Machine Scale Set (VMSS)

Compute Fleet

Arc Machines

+ Create

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Services

Group by no

mcd

Subscription equals all

Type equals all

Resource Group equals all

Location equals all

Add filter

Name	Subscription	Resource Group	Location	Status	Operating syst...	Size	Public IP address	Disks	Update status
ciscomcd-mcd-azure-lab-nrbcg	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...
ciscomcd-mcd-azure-lab-psprom	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...

- Confirme el estado de la puerta de enlace desde el panel MCD.

Summary

Cloud Details

Interfaces

Instances

Settings

Troubleshooting

Terraform

Availability Zone	Number of Instances
1	1
2	1

AVAILABILITY ZONES DETAILS

Refresh

Instance: 1

Instance Actions

Instance ID

/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999/resourceGroups/mcd_swesnitz/providers/Microsoft.Compute/virtualMachines/ciscomcd-mcd-azure-lab-psprorne

Instance Name

ciscomcd-mcd-azure-lab-psprorne

Datapath Private IP

Datapath 2 Private IP

Datapath 2 Public IP

-

Mgmt Private IP

-

Mgmt Public IP

-

State

● INIT

Created

2026-09-15 16:26:05.711 (LOCAL)

Last Heartbeat

NA

Image Version

10.0.0

Policy Updates

Please check cdFMC for policy update status.

Información Relacionada

- [Crear una VPC o VNet de servicio](#)
- [Procedimiento de integración de FTDv](#)
- [Configurar requisitos previos de gateway](#)
- [Descripción general de Multicloud Defense for Azure](#)
- [Cree y utilice un par de claves SSH público-privado para las VM de Linux en Azure](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).